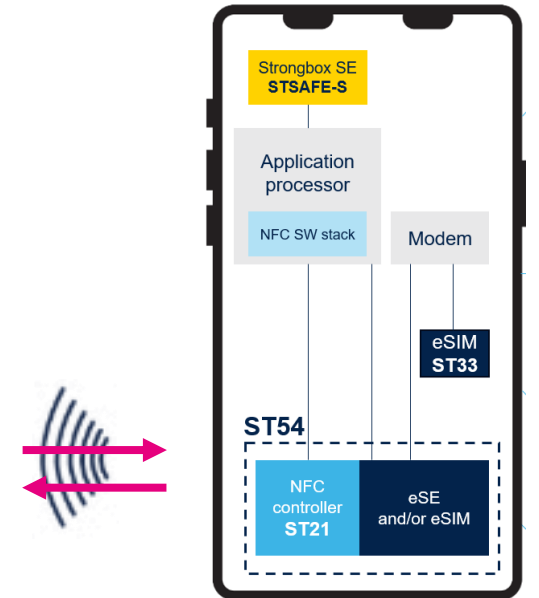
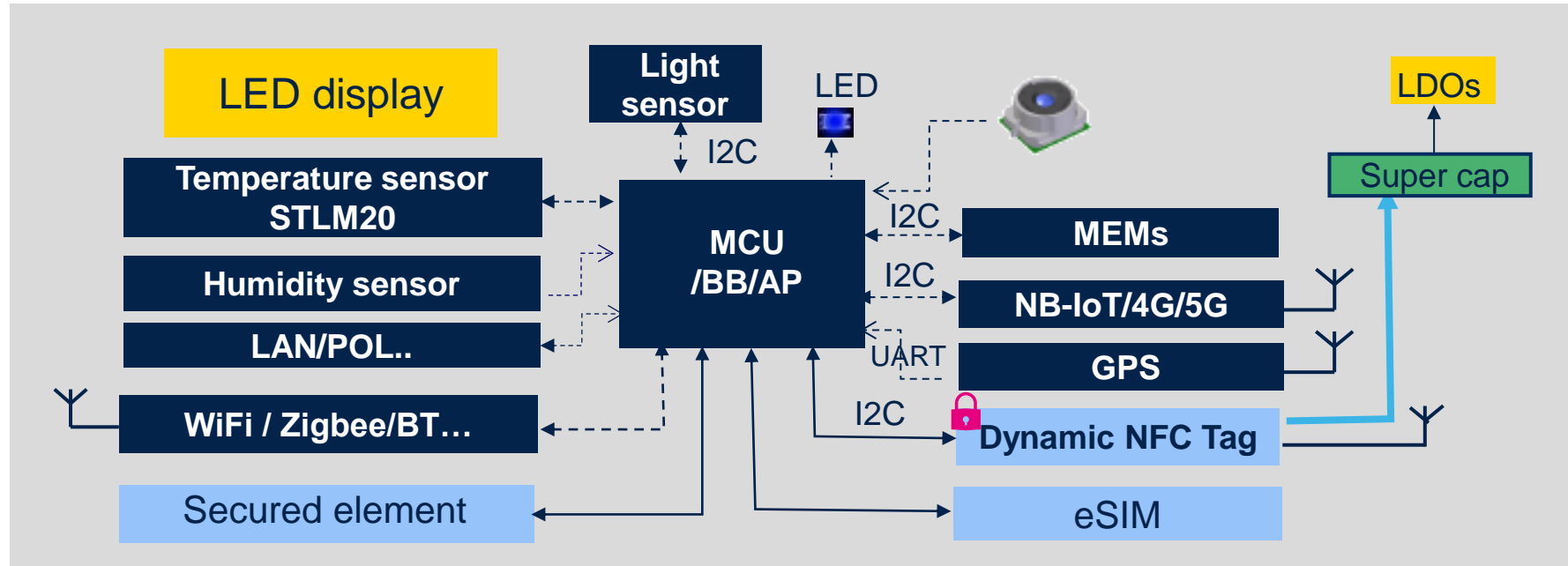


Enabling the next-gen connected experience: The role of eSIM and NFC controllers in smart devices

Kenneth Huang, Marketing Manager
STMicroelectronics

IoT smart devices



Cellular advantage:
 Long-range connectivity well-suited for IoT
 Ubiquity
 Reliability
 Security
 Power consumption

NFC advantage:
 UID: Identification
 No on-board power is needed for read/write of data → Good for PCB tracking
 Short read range: authorization, switch on / cut off control
 Easy to use: tap for BT / Wi-Fi pairing, data exchange



What is a SIM?

Subscriber Identity/Identification Module

1991

The SIM is an integrated circuit (IC) intended to securely store the international mobile subscriber identity (IMSI) number and its related key, which are used to identify and authenticate subscribers/mobile devices on a cellular network.

- The serial line is based the ISO-7816 specifications
- SIM features based on standard specification released by ETSI
- The data exchange protocol between SIM and modem is based on a poll-response protocols, exchanging “Application Data Packet Units” (APDU)
- The SIM performs the authentication to network by a challenge-response using a pre-shared secret keys that are known to the network
- The SIM performs also function related to the network operations

Starting with 3G, a more formal definition was introduced...

- The base HW and SW platform is the **Universal Integrated Circuit Card (UICC)**
- The network application running on top of the UICC is the **Universal SIM (USIM)**

Note

Form factor evolution



1991
1FF (ID-1)



1996
2FF (Mini)



2003
3FF (Micro)



2012
4FF (Nano)

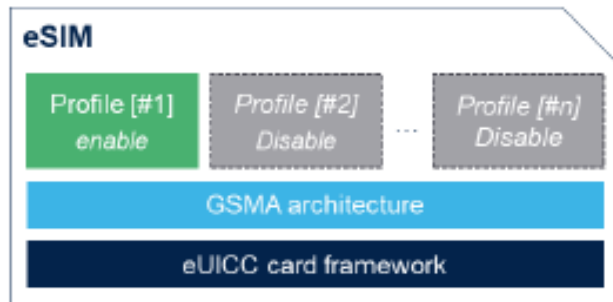


2016
MFF2 (DFN8 5x6)



GSMA eSIM concept

New standard product pushed by GSMA

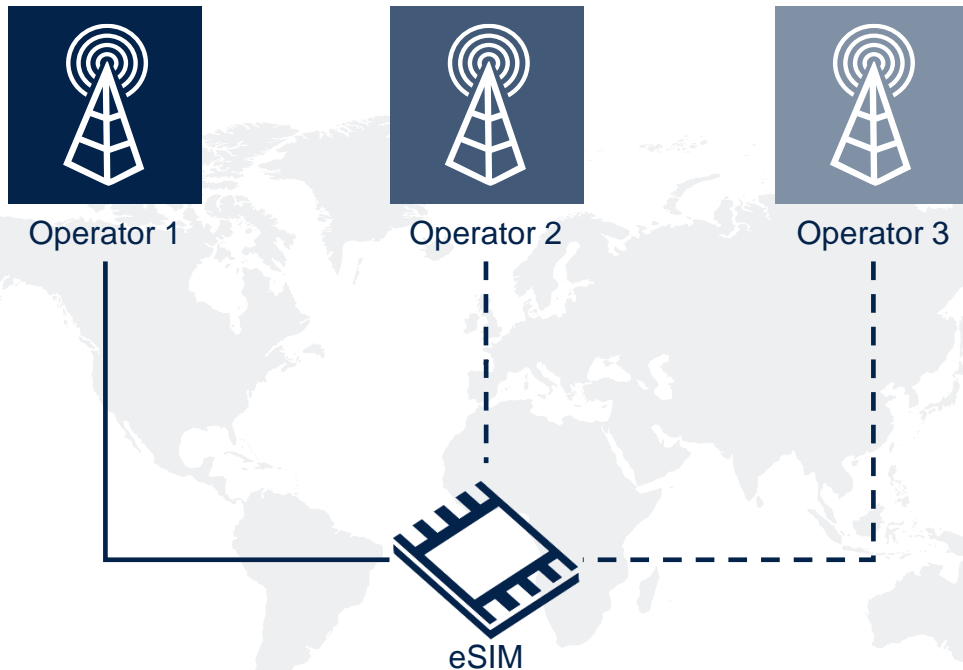


The **eSIM**, also known as an embedded UICC (eUICC), is a SIM

- Like a regular SIM is manufactured with a pre-loaded “bootstrap subscription” with out-of-the-box connectivity from Telecom Operator
- Offer the possibility to swap operator remotely without physical SIM replacement
- Hosts multiple operator profiles – only one at a time is enabled
- Is selected by OEM
- Available in multiple packages and HW grades

What is Remote SIM Provisioning (RSP)?

Over-the-air protocol for the remote management of operator profiles



Download profiles

Enable / Disable profiles

Delete profiles



Over 440 mobile operators already offer RSP across 120+ countries*

eSIM content and profile

eSIM content

類別	說明
IMSI (International Mobile Subscriber Identity)	國際行動用戶識別碼，唯一代表用戶身份 (例如：MCC + MNC + 使用者號碼)
Authentication Key (Ki)	用來與行動網路進行身份驗證的加密金鑰，極為機密
ICCID (Integrated Circuit Card Identifier)	SIM 本身的唯一識別碼 (不是用戶身份，是卡的編號)
本地網路資訊 (例如 MNC、MCC)	行動網路代碼與國家代碼，幫助設備選網
Operator Profile (營運商設定檔)	包含營運商的設定 (APN、網路類型、憑證等)
SMS、電話號碼存儲區	部分 eSIM 可儲存聯絡人、SMS (雖然現代裝置通常不這麼使用)
eUICC 軟體 (Embedded Universal Integrated Circuit Card)	控制和管理多個 eSIM 設定檔 (Profiles)，可以切換營運商

New

New

eSIM Profile

- Identifiers**
ICCID, IMSI, IIN, EID
- Authentication & Security(Profile protection)**
Authentication Key and OP/Opc, Security domains
Certificates/Key(for secure download & integrity)
- File system(Smaller size, modular delivery)**
These are elementary(EF) and dedicated files stored in the eSIM
- Applications**
3G/4G/5G subscription app, IMS/VoLTE services
STK applets(SIM toolkit menus, proactive commends)
- Operator Policies & Metadata(package size <50KB)**
Profile state(enable/disable), memory requirement
Fallback behaviour(in case of failure)
Policy rule(e.g., roaming restrictions, operator locks)
Service Provide Name(SPN) & brand display
- Network & Service Configurations**
PLMN lists for roaming, Emergency call configuration, IMS settings(for VoLTE, VoWiFi, IMS)


SGP.32

SGP.32

SGP.32

eSIM evolution: from M2M to Consumer to IoT

eSIM M2M



- Designed for unattended devices (no user interface)
- Server driven, push mode
- Centralized management of profiles


Service oriented



2014

GSMA SGP.01: eSIM Remote Provisioning Architecture
GSMA SGP.02: eSIM Technical Specification

eSIM Consumer



- Designed for consumer devices: smartphone, tablet, ...
- Client driven, pull mode
- Local management of profiles

User oriented



2015

GSMA SGP.21: eSIM Architecture Specification
GSMA SGP.22: eSIM Technical Specification

eSIM IoT



- Designed for network constrained devices (no SMS, no TCP/IP), with limited or no UI
- Server driven, push mode
- Centralized management of profiles

Service oriented



2022

GSMA SGP.31: eSIM IoT Architecture and Requirement Spec
GSMA SGP.32: eSIM IoT Technical Specification

ST33 eSIM: #1 in consumer eSIM

ST partners

- Partnership with major eSIM OS developers
- 276 MNOs over 118 countries ⁽¹⁾
- 300+ compatible eSIM Management Platform

Standards

- ST participation to key industry standards



ST positioning

Pioneer in Consumer eSIM deployment

ST market share: over 75% in 2023*

1+ Billion eSIMs shipped to date

Proven interoperability

Selected by all Tier1 OEMs

Android, iOS, Windows

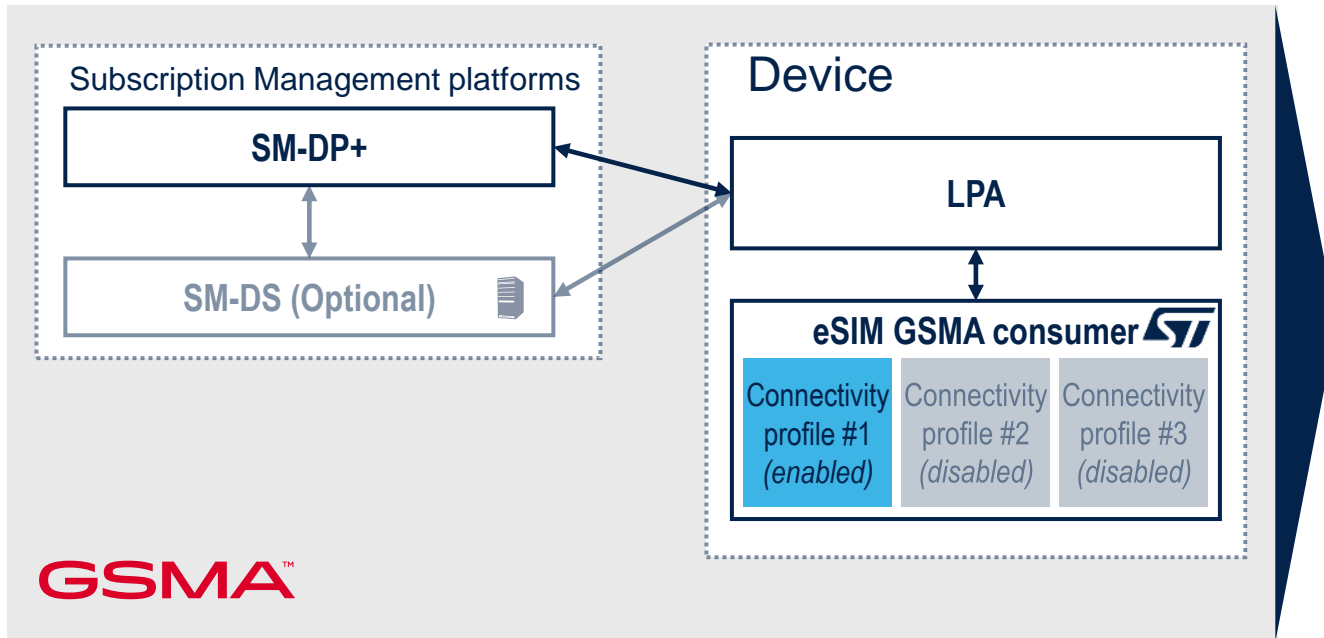
Multiple Enabled Profile (MEP) ready

Tiny WLCSP package

*Source: ST estimate

GSMA eSIM consumer overview

Secure, Scalable, and State-of-the-art architecture



OEM / customer benefits

Secure solution with a certified ecosystem

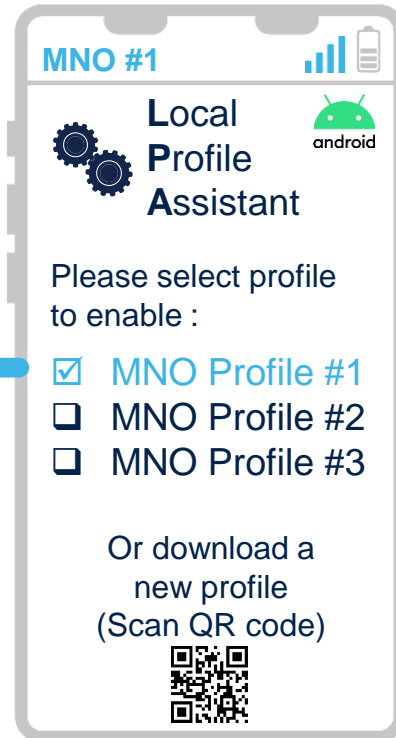
Scalable & Interoperable solution

Footprint optimized thanks to eSIM

Local profile assistant

The best end-user experience for profile management

17
Air



LPA services

- Scan QR code to download a profile
- Download and Install a Profile from the platform
- List all installed profiles
- Local Profile Management Operations (Enable / Disable / Delete...)
- Other additional eUICC information's (EID, Free memory,...)

User benefits

- SIM directly embedded into the device
- Connectivity selection is now fully digitalized
- Simplify the end-user experience

Introduction to GSMA for IoT specification

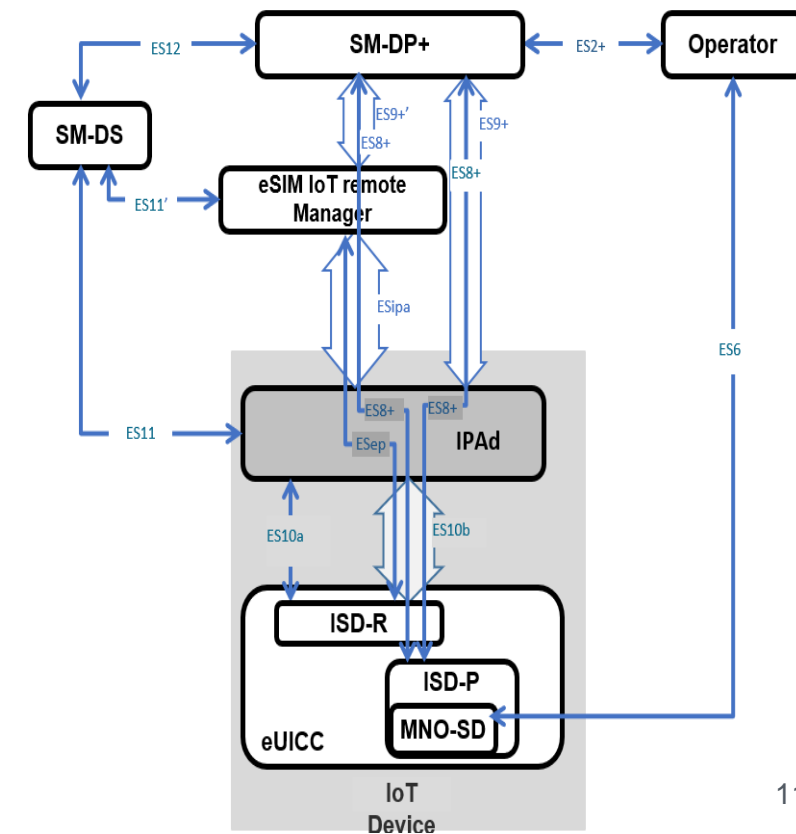
GSMA SGP.31/32

enables remote SIM provisioning of any IoT device

GSMATM

Benefits

- Like eSIM for Consumer
 - Operators manage the SM-DP+ server to store and send profiles to the devices
 - Remote provisioning can work on network without SMS (NB-IoT)
- Like eSIM for M2M
 - The profile download is initiated by Service Provider (Push mechanism)
 - Compatible with IoT devices having limited functionalities (no UI)
- Full control to OEMs to bring connectivity into their devices



This is a picture – to be replaced with real slide

ST4SIM(ST OS) complete portfolio

ST4SIM portfolio compatible with GSMA standards

GSMA™

ST4SIM-200x / 201x



- **4G/5G eSIM** compliant with:
 - ETSI & 3GPP Rel 13 / **Rel 16**
 - Java Card™ & GlobalPlatform™
- **Certified GSMA eUICC M2M** according to:
 - **SGP.02 v3.2**
 - **SGP.02 v4.2**
- **Multiple CPs available with Telecom Operators partner**

GSMA™

ST4SIM-CP2



- **4G eSIM** compliant with:
 - ETSI & 3GPP Rel 12
 - Java Card™ & GlobalPlatform™
- **Certified GSMA eSIM Consumer** compliant to:
 - **SGP.22 v2.2**
- Available with and without default Telecom Operator profile

GSMA™

ST4SIM-CP2_5G



- **5G eSIM** compliant with:
 - ETSI & 3GPP Rel 17
 - Java Card™ & GlobalPlatform™
- eSIM compliant to **GSMA SGP.22 v2.6**
- Available with and without default Telecom Operator profile
- **GSMA eSA certification**

GSMA™

ST4SIM-300



- **5G eSIM** compliant with:
 - ETSI & 3GPP Rel 17
 - Java Card™ & GlobalPlatform™
- eSIM compliant to **GSMA SGP.32 v1.2**
- Flexible bootstrap operator & eIM selection
- **GSMA eSA certification**

Available on multiple packages (card plug-in, MFF2, WLCSP) and chip hardware grade (Industrial, Consumer/IoT)

Unique full in-house capability to manage complete chain from chip design to the shipment for customers

ST4SIM-CP2_5G/ST4SIM-300

Features

- Remote SIM provisioning compliant with GSMA eSIM for IoT and TCA specification,
- Up to **7** connectivity profiles (depending on memory size)
- Compliant with 2G / 3G / 4G (LTE) /5G /CDMA / NB-IoT / CAT-M networks
- OTA capability over **SMS, CAT-TP & HTTPS** (including DNS)
- Multi-interfaces able to combine eSIM + eSE
- ETSI, 3GPP and 3GPP2 release **17**(API Rel16)

Hardware

- Product available on **ST33K1M5M**
- ST33 product based on a 32-bit Arm® Core®-M35P CPU core
- Asynchronous serial I/O port ISO/IEC 7816-3 compatible
- Operating temperature: -40°C to +105°C
- Common Criteria **EAL6+**

Security

- Symmetric cryptography and asymmetric cryptography RSA
- HTTPS remote management TLS v1.0, V1.1 and v1.2



VFD8P8
6 x 5 mm, wettable
flanks (MFF2)



WLCSP24

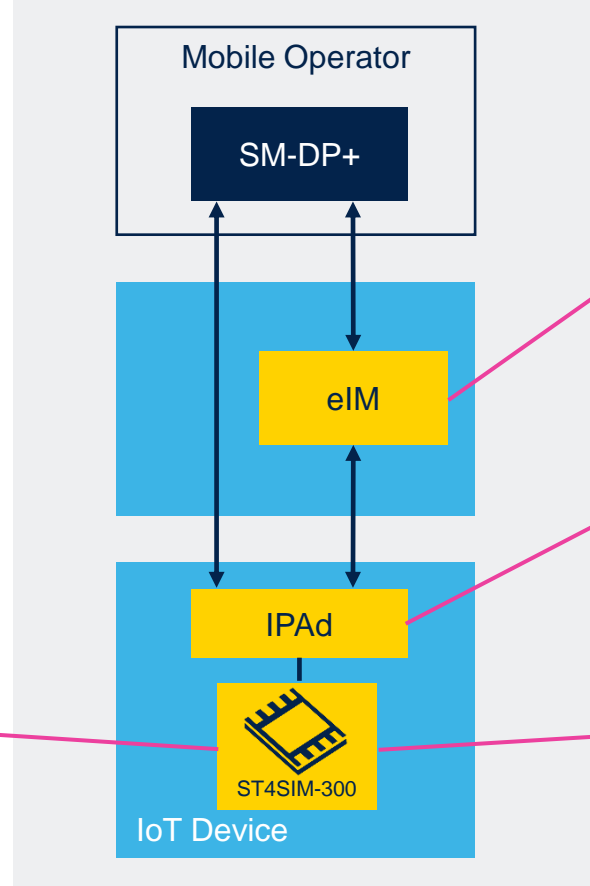
ST4SIM 300 - Ecosystem

Complete ecosystem built around a cutting-edge eSIM for IoT

Building blocks:

- eSIM – ST4SIM-300
- (optional) bootstrap connectivity
- IPA – IoT Profile Assistant
- eIM – eSIM IoT Remote Manager

ST4SIM-300
eSIM for IoT (GSMA SGP.31/SGP.32)



eIM

Connectivity management services offered through partners

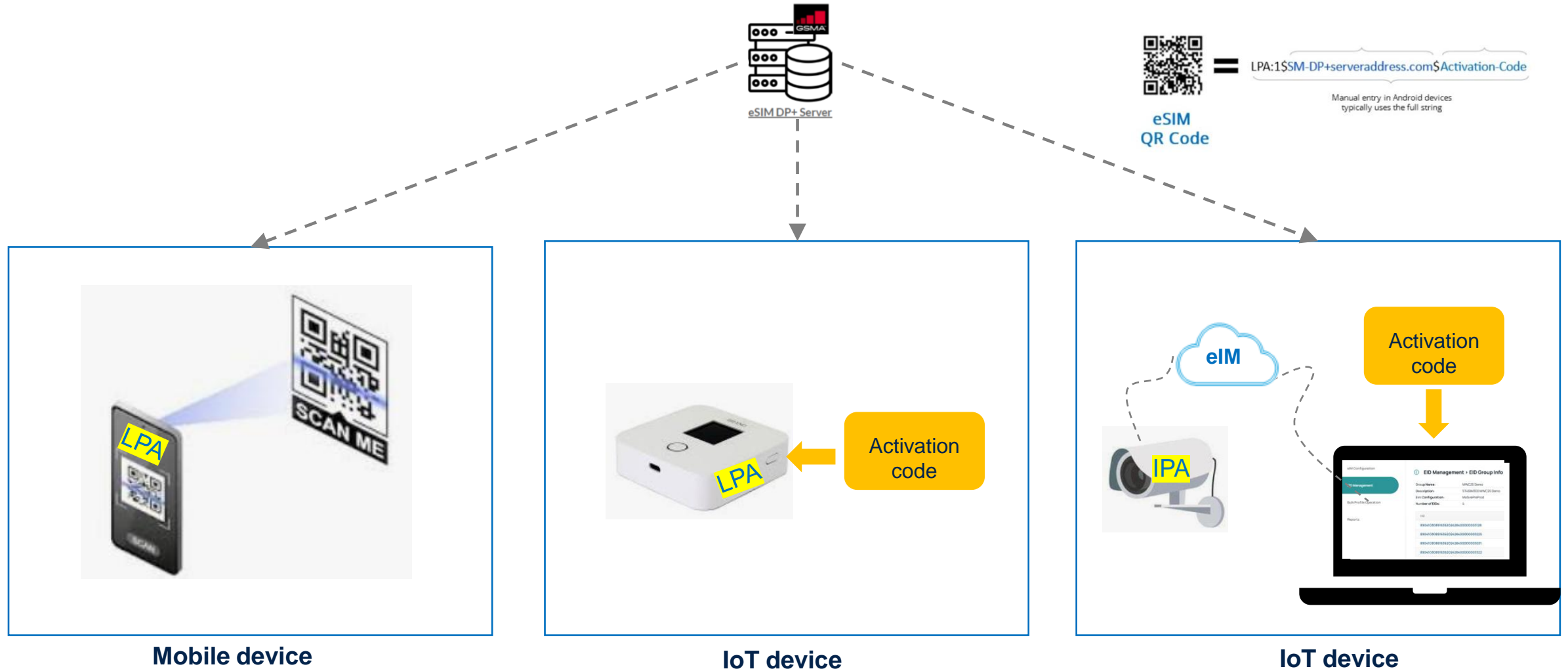
IPAd

Reference implementation for STM32
Source code available in C language

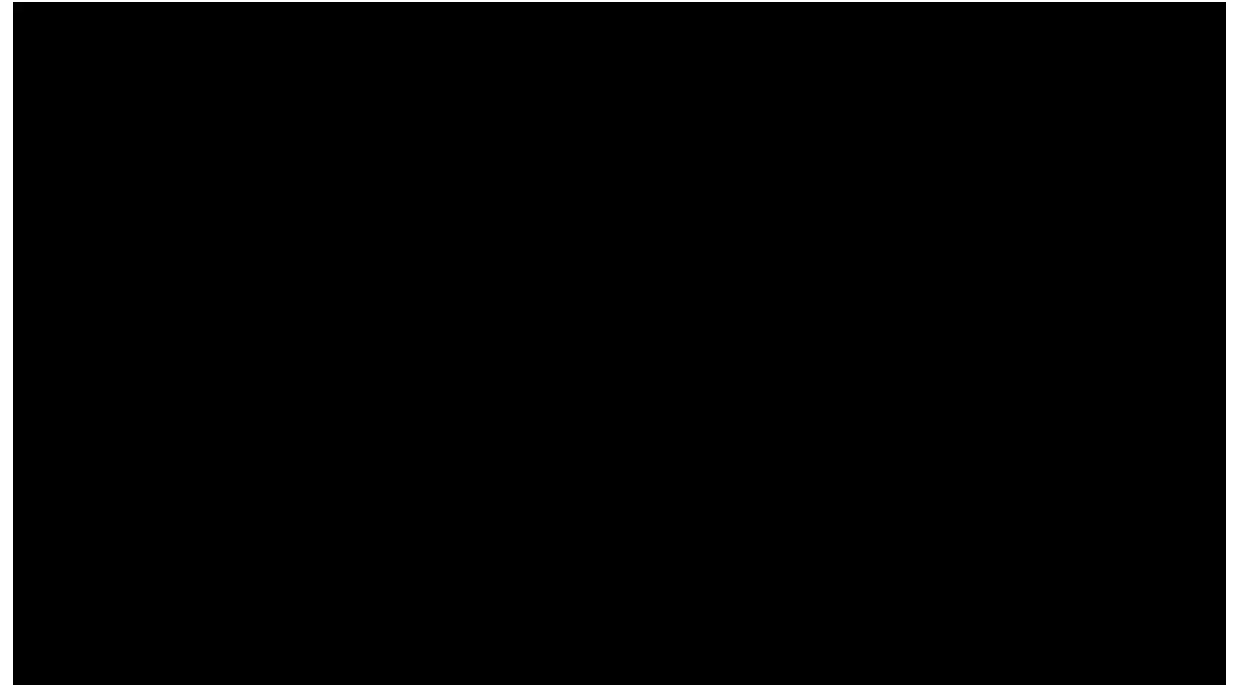
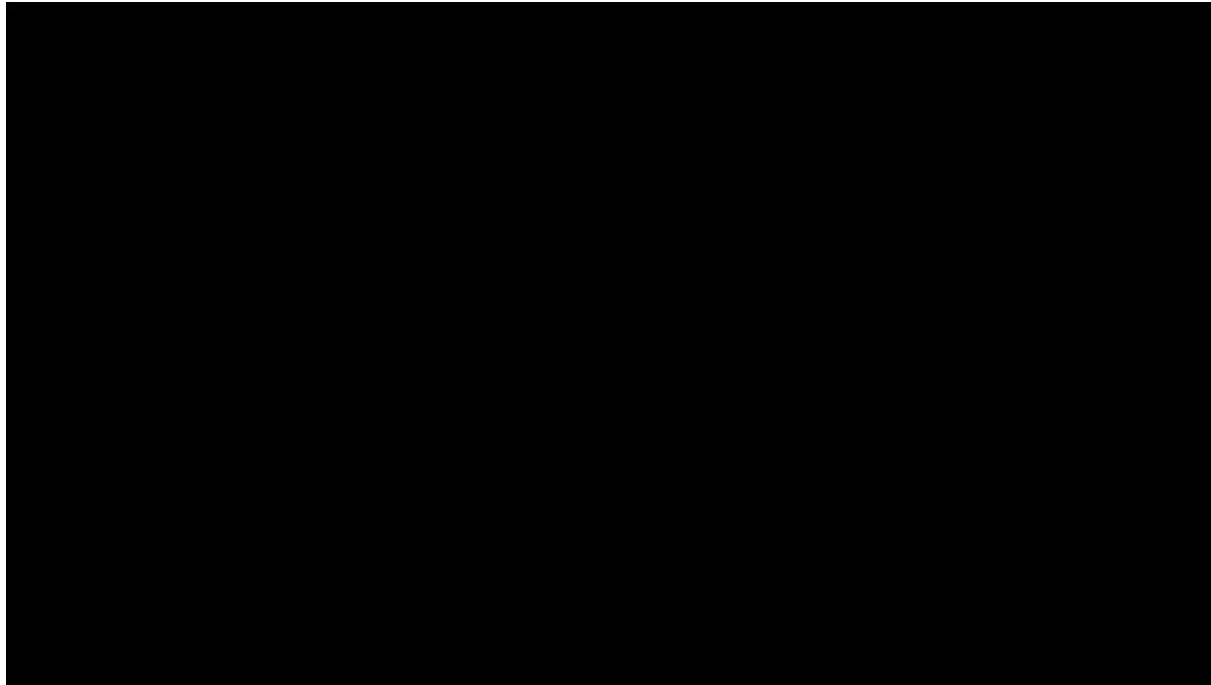
Bootstrap connectivity

Optional pre-loaded connectivity profile
On-demand profile development

RSP profile download for end device

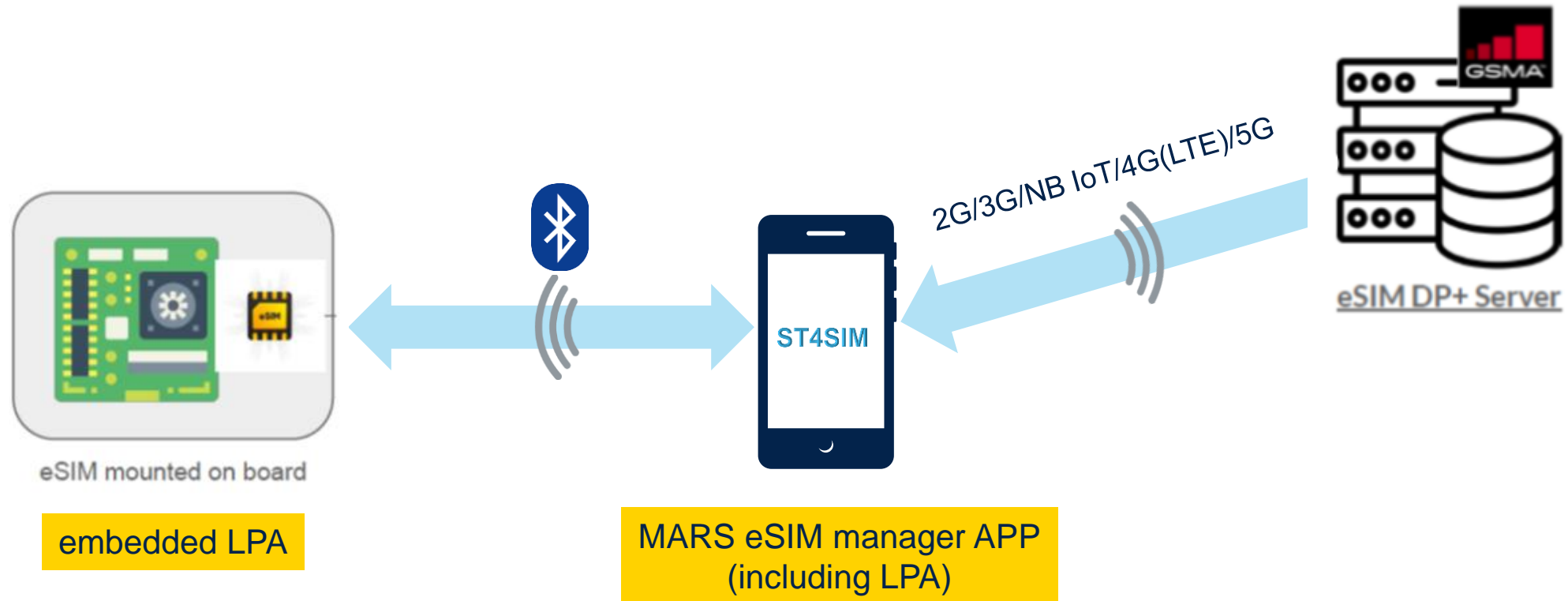


Profile download through eIM demo

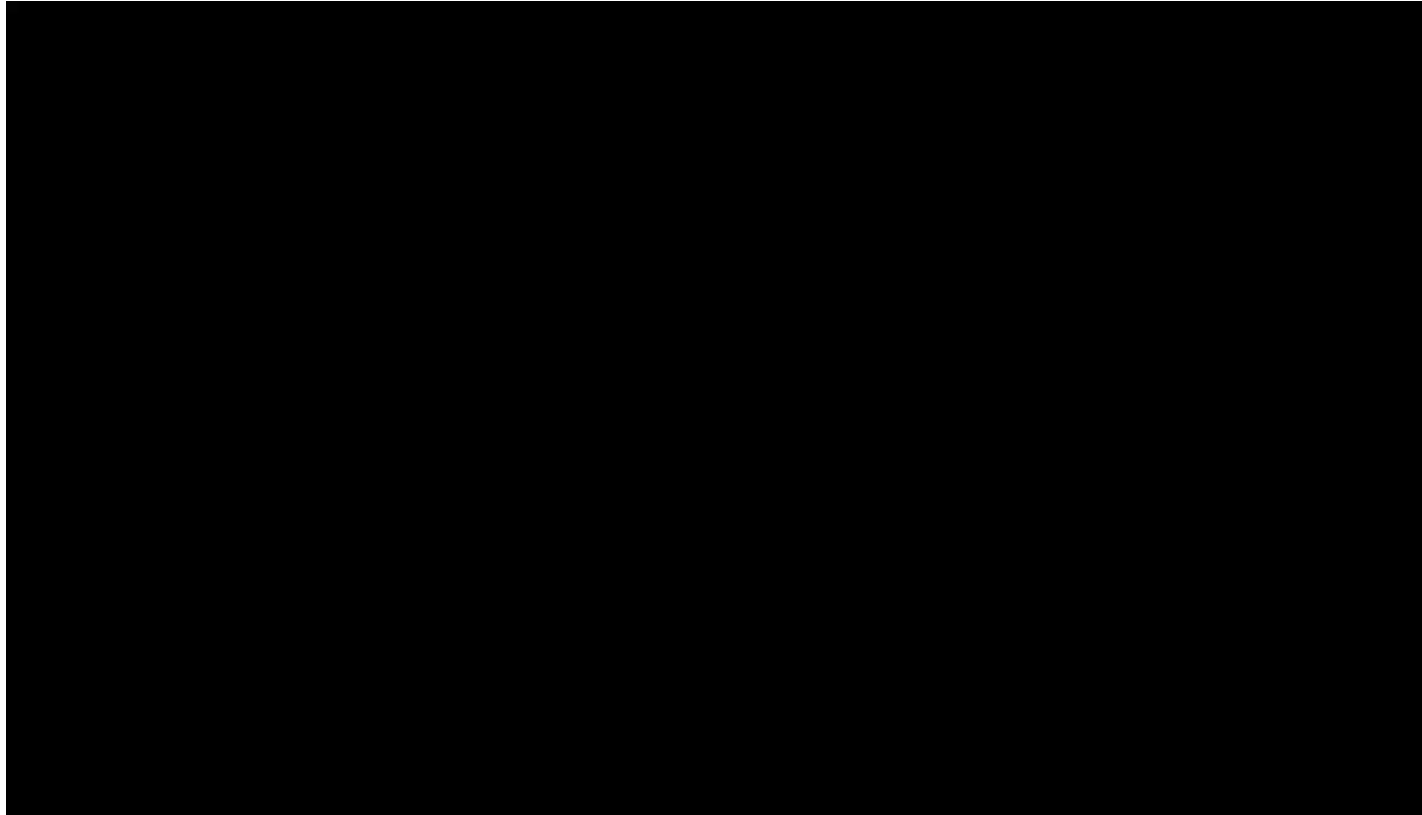


<https://www.marsesim.com/zh-tw/business>

eSIM profile download through a mobile phone



Profile download through BT demo



<https://www.marsesim.com/zh-tw/business>

ST4SIM profile package

eSIM consumer

P/N

ST4SIM-CP2_5G
ST4SI5M005200HL9

ST4SIM-CP2_5G
ST4SI5M004700HFW



eSIM M2M/IoT

P/N

ST4SIM-300
ST4SI3M004800HL9

ST4SIM-300
ST4SI3M004600HFW

4FF ST4SIM-300
ST4SI3M005000A84

Mars eSIM

**Global approach
Fixed rate for IOT
connection traffic**

Free of uncertain cost issue!

01	02	03	04
<p>5年方案 試點起步</p> <ul style="list-style-type: none"> 流量：250 MB SMS：120 封 費用：\$ 7.5 USD起 覆蓋範圍 	<p>10年方案 穩定成長</p> <ul style="list-style-type: none"> 流量：550 MB SMS：250 SMS 費用：依需求報價 覆蓋範圍 	<p>15年方案 擴張深耕</p> <ul style="list-style-type: none"> 流量：750 MB SMS：350 SMS 費用：依需求報價 覆蓋範圍 	<p>20年方案 全球布局</p> <ul style="list-style-type: none"> 流量：1,200 MB SMS：500 SMS 費用：依需求報價 覆蓋範圍

Long effective period support for IoT devices: 5、10、20 years

ST4SIM – Industrial / M2M / IoT target segments

Asset management (asset tracking / PDAs)

Energy management (all meters / building automation / smart grid)

Security management (home security & automation / video surveillance)

Location tracking (fleet management / OEM-aftermarket telematics / people & pet tracking / heavy transport vehicles & equipment)

Monitoring status (home appliances / usage-based insurance)

Smart cities (smart parking / smart street lighting)

Healthcare (patient monitoring (wearable and not) / diagnostic equipment)

ATM/POS/Vending/Kiosks

Agriculture (environmental connected sensors / low mobility machines)



STSAFE™ family secure element

Security certified solutions from IoT nodes to IoT infrastructure

HW CERTIFIED CC EAL5+

Optimized

STSAFE-A

- Fixed features set:
 - Authentication
 - Secure connection establishment
 - Secure storage
 - LPWAN LoRa / Sigfox compliant
- Personalization services
- Seamless integration with STM32 ODE package

CERTIFIED CC EAL4+, TCG 2.0, FIPS140-3

Standardized

STSAFE-TPM

- Platform integrity
 - Secure Boot
 - Secure Firmware upgrade
- Trusted network access
- Secure storage
- Linux based MPU Development kit



HW CERTIFIED CC EAL6+

Flexible

STSAFE-S

- Javacard based OS
- Application:
 - Android Weaver
 - Secure storage
 - Android Keymint
- Support for GlobalPlatform™ SCP03 and SCP11
- Secure personalization





Android security history

“The availability of a **TEE** offers an opportunity for Android devices to provide hardware-backed, strong **security services** to the Android OS, to platform services, and even to third-party apps”. KeyMaster is the TEE App delivering the service within Android (Keystore).

Google **recommend the usage of a discrete** processor in Advanced Assurance Program (**AAP**) launched in 2018

Google introduce **Tamper resistant discrete** component in Pixel 3 phones with Titan

Since 2018, Google leverages on tamper resistant element to ensure device security. They prepared Android ecosystem with the support of TEE and SE. The trend is now clearly in favor of SE.

← 2014 Android 5 2015 Android 6 2016 Android 7 2017 Android 8 →

← 2021 Android 12 2022 Android 13 2023/24 Android 14/15 →



KeyMaster

provides simple crypto services: digital signing and verification operations

KeyMaster 1

supports symmetric primitives

KeyMaster 2

supports key attestation and version binding

KeyMaster 3

supports hardware attestation

KeyMaster 4

supports embedded secure element

KeyMaster 4 as **Secure Element Applet is called Strongbox**

Strongbox HAL is Google AOSP

Android Ready SE

program launched

KeyMint

replaces KeyMaster

Strongbox KeyMint **strongly recommended**

Strongbox KeyMint

mandatory for device equipped with eSE

Strongbox for Mobile

KeyMint

2022  2023 

Hardware backed attestation for premium apps
Secure provisioning of Android keys

- Offer a set of Android APIs to Applications to manage cryptographic credentials and operations
- Shall run in an environment with a discrete CPU, secure storage, a high quality true random number generator, tamper resistant packaging, and side channel resistance

Weaver

2022  2023 

A password-protected data storage

- User can store secrets (like fingerprints or swipe pattern) and associate them with a password
- To read secrets, user needs to present the valid password
- Weaver supports countermeasures for brute force attacks

- Offer to Consumer device a secure service integrated in Google Android environment, part of Android SE program
- Various integration in phones possible
- 3 ST Strongbox implementations available
 - ST54
 - standalone secure element STSAFE-S320
 - standalone eSIM ST33

STSAFE-S320 key product features

Hardware features

- Arm® Cortex®-M35P 32-bit RISC core cadenced at 70Mhz
- Operating temperature range : -30°C to 85°C
- High-stress memory (HSM)
 - 200,000 Erase/Write cycles endurance
 - 10 million write cycles for specific data
 - 15 years data retention at 850C
- Available in WLCSP24
- External interfaces
 - Slave serial interface SPI Slave (up to 10 MHz)
 - Slave I²C interface up to 1 Mb/s
- Class C (1.8V), class B (3V) and 3.3V supply voltage ranges
- ESD protection greater than 4kV



Hardware features

- Java Card™ 3.0.5 Classic operating system
- GlobalPlatform™ 2.3 support
- Support for GlobalPlatform™ SCP03 and SCP11
- Support for GlobalPlatform™ executable load file (ELF) upgrade
- Dynamic memory management
- APDU communication over I²C/SPI based on the GlobalPlatform™ “APDU Transport over I2C/SPI” specification
- Firmware upgrade mechanism

Application

- Android Weaver
- Secure storage
- Android Keymint v2 (Android 14) & v3 (Android 15)

ST25 NFC / RFID portfolio

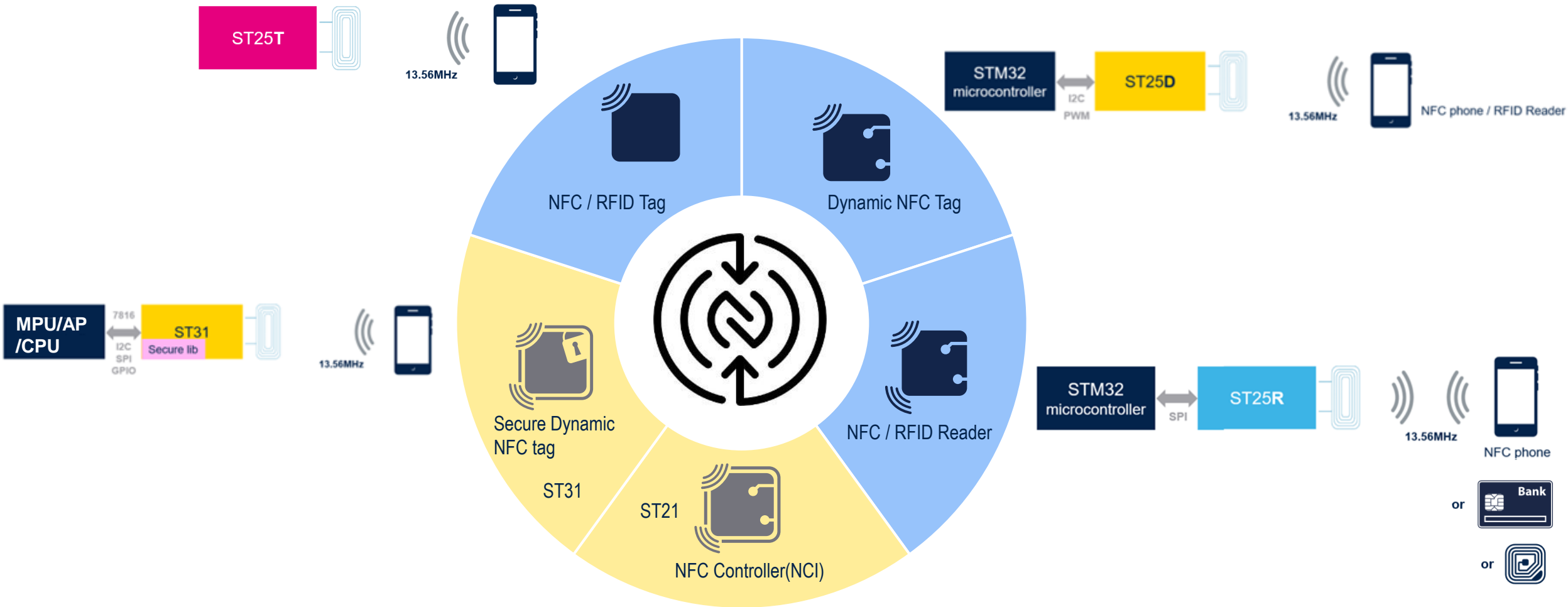
one-stop-shop for tags and readers

Tags					Dynamic tags			Readers			
ST25TA	ST25TA-E	ST25TB	ST25TN	ST25TVC	M24SR	ST25DVC-I2C *	ST25DV-PWM	ST25R200 ST25R100	ST25R3916B ST25R3917B	ST25R300	ST25RN300
ISO14443-A 106 kbps NFC type 4	ISO14443-A 106 kbps NFC type 4	ISO14443-B 106 Kbps	ISO14443-A 106 kbps NFC type 2	ISO15693 up to 53 Kbps NFC type 5	ISO14443-A 106 kbps NFC type 4	ISO15693 up to 53 kbps NFC type 5	ISO15693 up to 53 kbps NFC type 5	ISO14443-A/B ISO15693	ISO14443-A/B ISO15693 Felica ISO18092	ISO14443-A/B ISO15693 Felica ISO18092	ISO14443-A/B ISO15693 Felica ISO18092
EEPROM 512b - 64Kb 200-year retention 1M cycles	Flash 2Kb 25-year retention 500k cycles	EEPROM 512b-4Kb 40-year retention 1M cycles	EEPROM 512b-1.6Kb 40-year retention 100k cycles	EEPROM 512b-64Kb 60-year retention 100k cycles	EEPROM 2Kb-64Kb 200-year retention 1M cycles	256B buffer EEPROM 4Kb-64Kb 40-year retention 1M cycles	EEPROM 2Kb 40-year retention 100k cycles	Reader/Writer	Reader/Writer P2P Card Emulation	Reader/Writer P2P Card Emulation EMVCo® & PBOC	Reader/Writer P2P Card Emulation
TruST25 digital signature 128b password 20b counter UID RF Field Detect	Augmented NDEF Edge TruST25 digital signature ECC crypto engine 4-digit UTC 24b counter UID	32b counter Lock OTP bits UID	Augmented NDEF TruST25 digital signature 24b UTC UID	Augmented NDEF TruST25 digital signature 64b password 24b UTC UID Tamper Detect	128b password RF disable RF Detect UID	Fast X-fer Mode 64b password E-harvesting RF Detect UID	TruST25 digital signature 64b password UID	Dynamic Power Out (DPO) OverShoot Protection (OSP) Dual-antenna	Active Wave Shaping (AWS) Dynamic Power Out (DPO) Auto Antenna Tuning (AAT) Dual-antenna	Active wave shaping (AWS+) Dynamic Power Out (DPO+) Auto Antenna Tuning (AAT) Dual-antenna	NFC Controller Interface (NCI) Active wave shaping (AWS) Dynamic Power Out (DPO) Active Load Modulation (ALM)
					I2C 1MHz 2.4V-5.5V	I2C 1MHz Write 16B page 1.8V-5.5V	2x PWM 488-31.25 kHz 1.8V-5.5V	SPI 10 / 6Mbps 2.7V-5.5V 1.2W - 0.8W	SPI 10Mbps I2C 3.4Mbps 2.4V-5.5V 1.6W	SPI 10Mbps 2.7V-6.0V 2.2W	I2C 1MHz 2.5V-5.1V 2.2W
SBN12 / SBN075 / FPN5	SBN14 / SBN075	SBN12 / SBN075	SBN12 / SBN075 / FPN5	SBN12 / SBN075 / FPN5	SO8 / TSSOP8 / FPN8 / SBN12	SO8 / TSSOP8 / FPN8 / FPN12 / WLCSP10	SO8 / TSSOP8	24-pin TQFN	32-pin QFN / WLCSP-36	32-pin QFN	WLCSP-49



*: successor of M24LR
and ST25DV-I2C

NFC products





ST25D dynamic NFC tag overview

Mass market device, right fit for industrial & consumer applications

Key features

- NFC Forum Type 5 / Type 4
- I2C 1MHz
- EEPROM up to 64kb + Buffer 256B
- Energy Harvesting
- Robustness (up to 105°C, 10 years)
- Easy integration (small packages)
- Interoperability with major brands

Applications



Connected Home



Medical



Metering



Lighting



Appliance



Electronic Shelf Label

Products

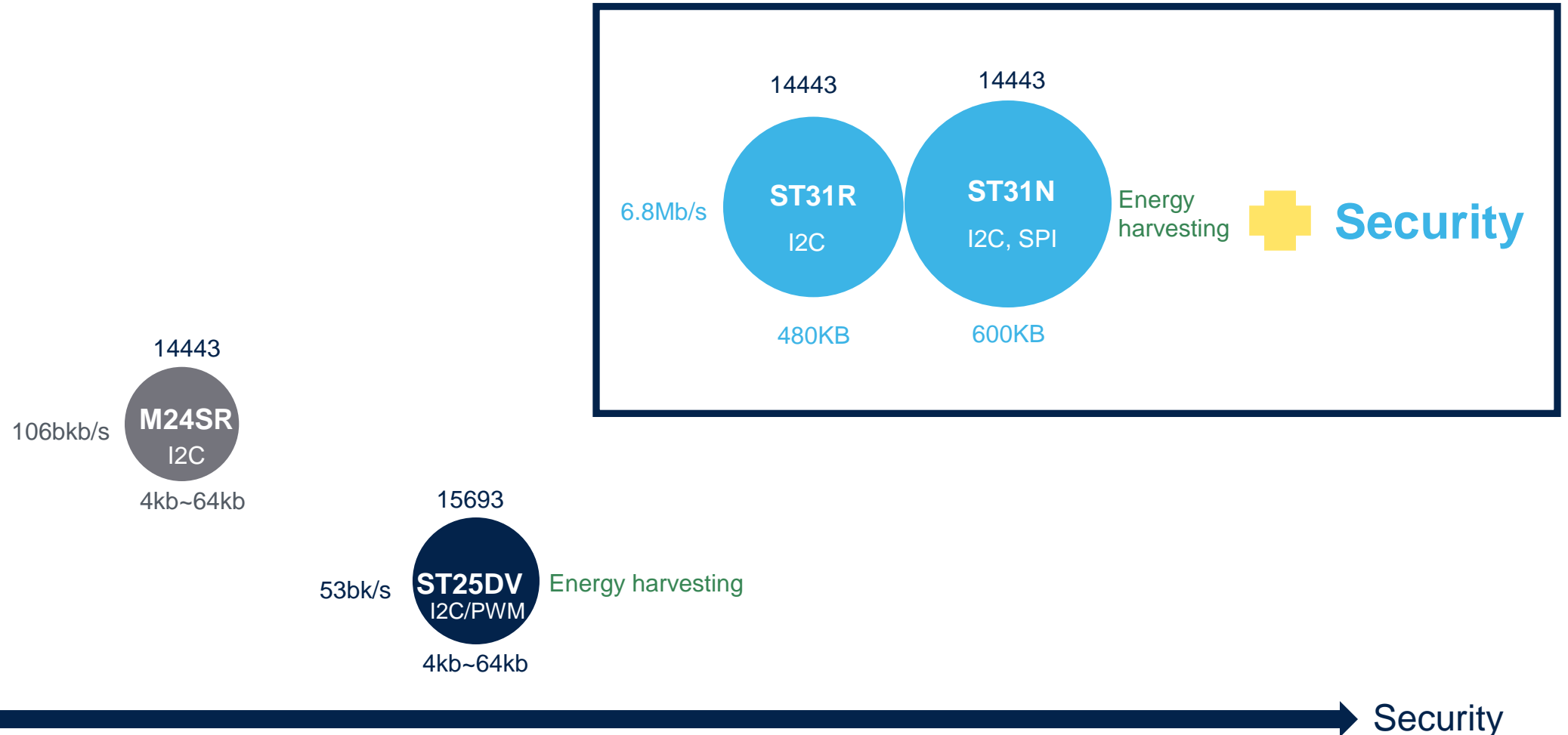
NFC Tag type 5
With PWM
ST25DV-PWM

NFC Tag type 5
Enhanced & I2C
ST25DVC-I2C / ST25DV-I2C

NFC Tag type 4
I2C
M24SR

Dynamic tag

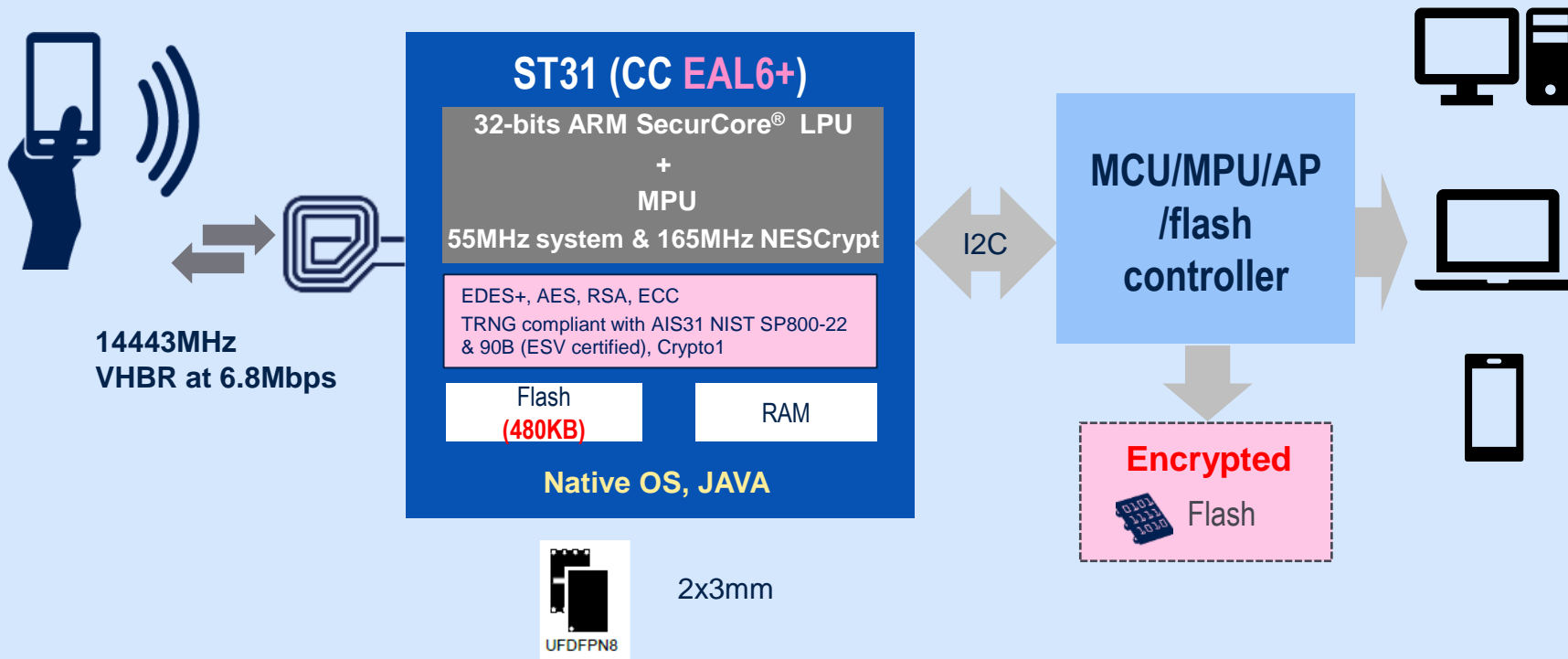
Data rate



ST31 secured dynamic tag

High performance and security but cost-effective NFC dynamic tag

Use NFC phone to lock/unlock Flash





ST25R reader overview

Right fit for industrial & consumer applications

Key features

- NFC Forum Certified device
- 1.6W Highest Output Power
- Active Waveshaping
- Dynamic Power Control
- Noise Suppression Receiver
- Automatic Antenna Tuning
- Interoperability with major brands

Applications



Payment terminals



Healthcare & beauty



EV Charging



Smart Home



Ki cordless



Power tools, gaming

Products

NFC Reader & P2P
EMVCo - PBOC
ST25R3911B / 12

NFC Reader, CE & P2P
EMVCo - PBOC
ST25R3916B / 17B / 19B

NFC Reader, CE & P2P
ST25R3918

NFC Reader, Writer
ST25R100 / ST25R200



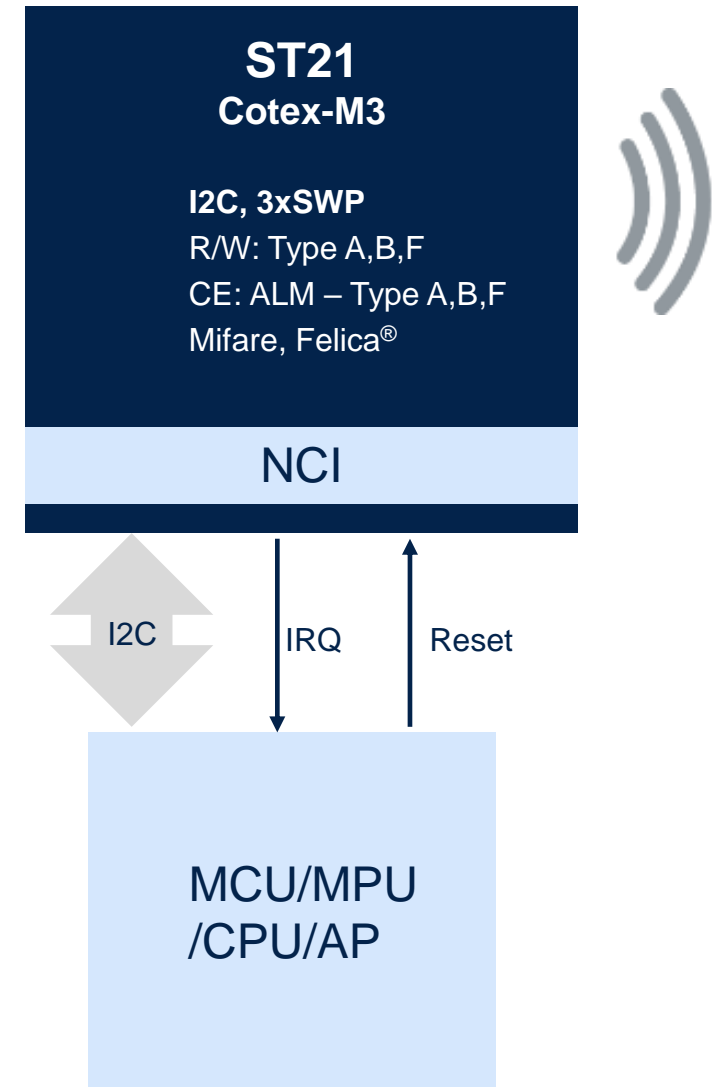
ST21 NFC controller(NCI) solutions

ST21 Benefits

- Standalone NFC NCI controller
- Volume production at major OEMs
- Best-in-class RF performance

Key applications

- Mobile ticketing
- Mobile payment
- Access control



ST54 NFC + Secure Element solutions

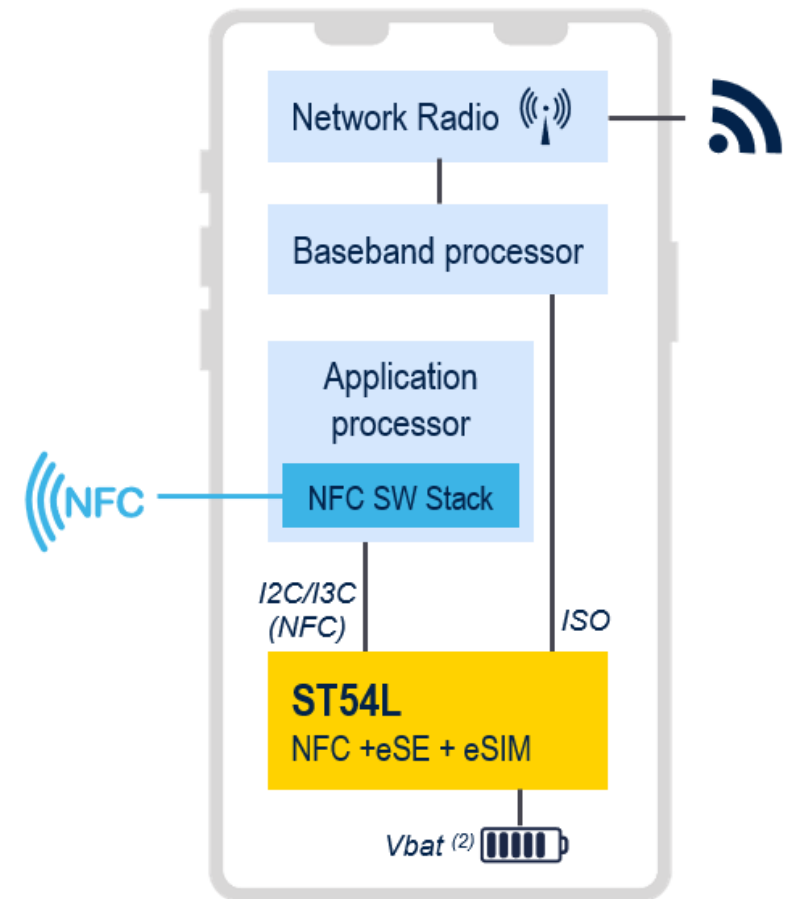
Reference solution in Android ecosystem

ST54 benefits

- #1 Felica, MIFARE® integration in Android framework
- Flexible configuration, NFC + (eSE &/or eSIM)
- Reduced bill of material and power consumption

Key applications

- Mobile ticketing
- Mobile payment
- Digital Car Key



ST54L key product features

Flexible offering to support NFC+eSE, NFC+eSIM and NFC+eSE+eSIM

HW benefits

- 1st eSE on the market powered by 115Mhz ARM® Cortex®-M35P
- 1.2V I/O support
- Bigger user memory in eSE **3.3MB**
- Faster transactions
- RW and CE distances increased
- Improved factory tests modes

Supported certifications schemes

- **EMVCo**, CC, GSMA eSA, CCC rev3, FeliCa® Network, MTPS

External UWB chipset

- Integrated with QORVO QM35
- Integrating with **Qualcomm** SM8750 + RI F/WiFi/I IWR Chin

Trusted eSIM

- 350+ Mobile Network Operators
- 100+ countries
- Support of Non-Terrestrial Network

GSMA



Supported technologies & use cases

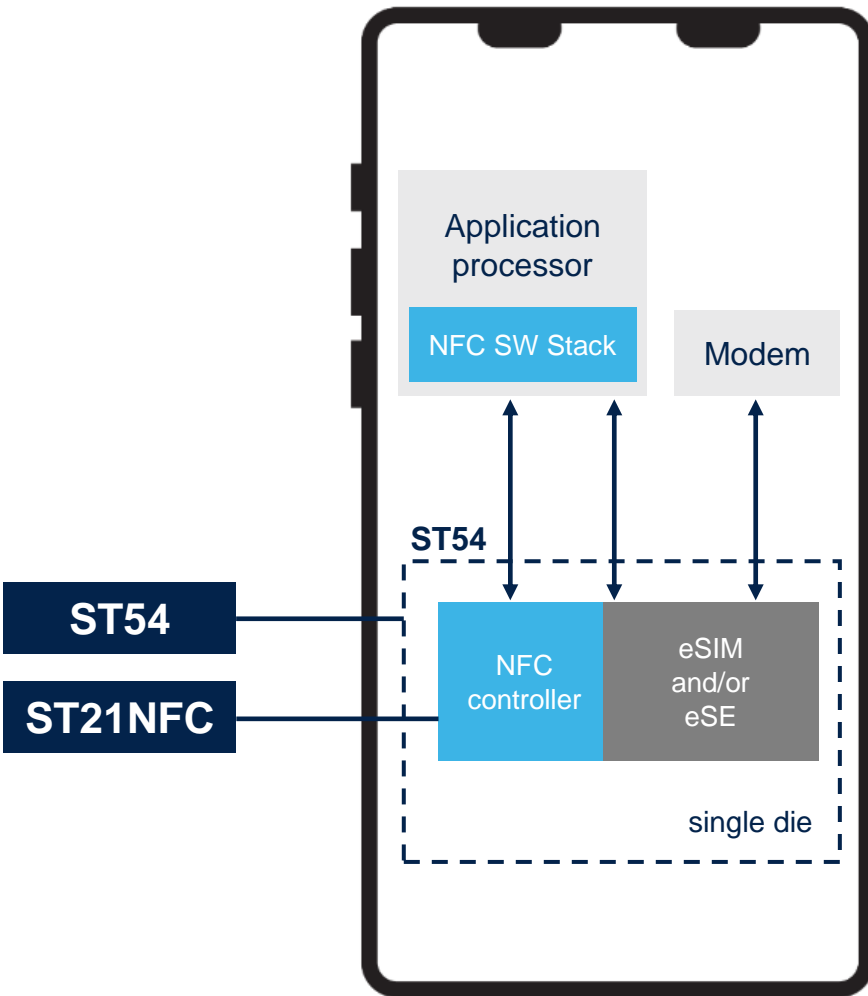
- MIFARE®
- Calypso
- Cipurse™ (OSPT)
- FeliCa® HK, Japan
- China Transit
- Fundan Transit
- UWB secure ranging
- eSIM
- NFC Charging Rx / Tx
- Japan eID
- OFL (T=1) for TEE integration
- **ECP**

THALES



- eSIM Multiple Enabled Profile
- NFC eSIM (CAT3)
- Smart access control
- Digital Car Key
- Strongbox (Weaver + Keymintv2/v3)
- German eID

ST54 Family



Several configurations

ST54

Convergence / Combo

NFC + eSE + eSIM

NFC + eSIM/eSE

NFC + eSIM

NFC + eSE

ST21NFC

NFC standalone

NFC



Pin-to-pin compatibility

Our technology starts with You



Find out more at www.st.com

© STMicroelectronics - All rights reserved.

ST logo is a trademark or a registered trademark of STMicroelectronics International NV or its affiliates in the EU and/or other countries.

For additional information about ST trademarks, please refer to www.st.com/trademarks.

All other product or service names are the property of their respective owners.

